NESEC
Gesellschaft für angewandte Netzwerksicherheit mbH

Hacking SCADA/SAS Systems

Used Techniques, Known Incidents and Possible Mitigations

Seminar at Petroleum Safety Authority Norway
at 29/11-2006

Christian H. Gresser
cgresser@nesec.de

Agenda

- About NESEC
- What is SCADA
- Well-known Incidents
- IT-Security and control Systems
- Problems in SCADA security
- SCADA systems security is different
- Hacking is easy
- IT-security in the future
- Possible solutions
- Lessons learned

About NESEC

- Founded 2002 as a system integrator specialized on IT security in Freising (near Munich/Germany)
- Strong focus on security in production environments
- Close cooperation with ABB Automation Products, development of security concepts and solutions for ABB customers
- Security analysis and penetration tests, even in life production, to identify possible threats and rate risks
- Working solutions to secure production plants and SCADA systems without interruption in production
- Customers include Munich Airport, Krupp-Mannesmann steel production, Volkswagen, Altana Pharma, and more

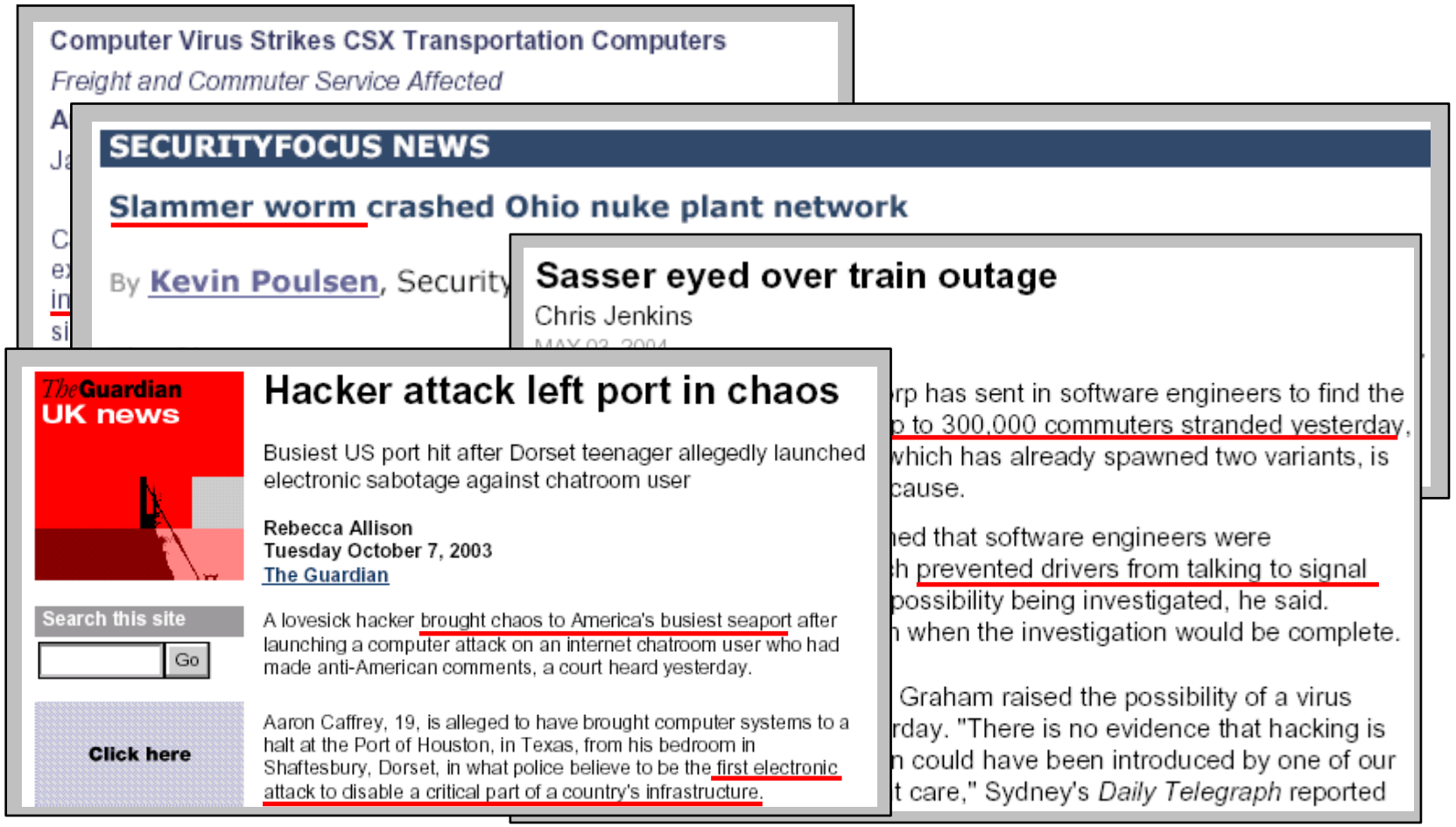
SCADA

- „Supervisory Control and Data Acquisition“
- Monitor and control industrial systems
  - Oil and Gas
  - Air traffic and railways
  - Power generation and transmission
  - Water management
  - Manufacturing
  - Production plants
- Huge threats
  - Massive power blackout
  - Oil refinery explosion
  - Waste mixed in with drinking water

What is SCADA and control systems?

- The power in your home
- The water in your home
- Where the wastewater goes
- The cereals and milk for breakfast
- Traffic lights on the way to the office
- The commuter train control system
- The phone system to your office
- The air conditioning in your office building
- The convenience food in the canteen
- much, much more …

Well-known Incidents



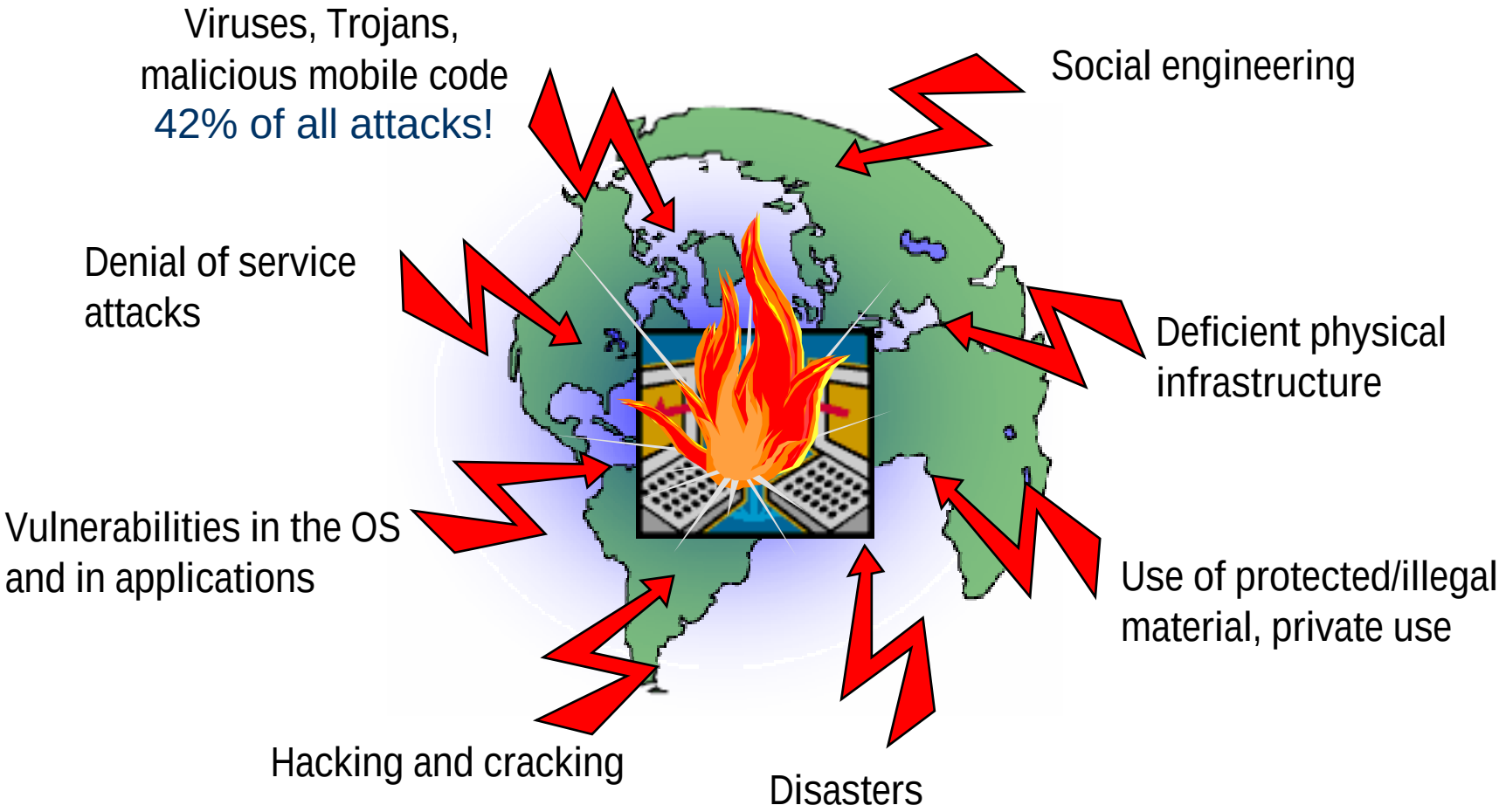
Well-known Incidents

- Aaron Caffrey, 19, brought down the Port of Houston October, 2003. This is thought to be the first well-documented attack on critical US infrastructure.
- In August 2003, computer systems of CSX Transportation got infected by a computer virus, halting passenger and freight train traffic in Washington, DC.
- In 2003, the east coast of America experienced a blackout, while not the cause, many of the related systems were infected by the Blaster worm.
- Computers and manuals seized 2003 in Al Qaeda training camps were full of SCADA information related to dams and related structures
- Ohio Davis-Besse nuclear power plant safety monitoring system was offline for 5 hours due to Slammer worm in January 2003
- 2001, hackers penetrated a California Independent System Operator which oversees most of the state's electricity transmission grid, attacks were routed through CA, OK, and China.

Well-known Incidents

- In 2000, former employee Vitek Boden release a million liters of water into the coastal waters of Queensland, Australia
- A Brisbane hacker used radio transmissions in 2000 to create raw sewage overflows on Sunshine coast
- In 2000, the Russian government announced that hackers succeeded in gaining control of the world‘s largest natural gas pipeline network (owned by Gazprom)
- In 1997, a teenager breaks into NYNEX and cuts off Worcester Airport in Massachusetts for 6 hours, affecting both air and ground communications.
- In 1992, a former Chevron employee disabled it‘s emergency alert system in 22 states, which wasn‘t discovered until an emergency happened that needed alerting.

Risks in Production Environments



Attacker‘s SCADA Knowledge

- Ethernet
- TCP/IP
- Windows
- RPC
- SMB
- 802.11b
- HTTP/HTTPS
- ASCII
- Unix/Linux/Solaris
- TFTP
- SQL

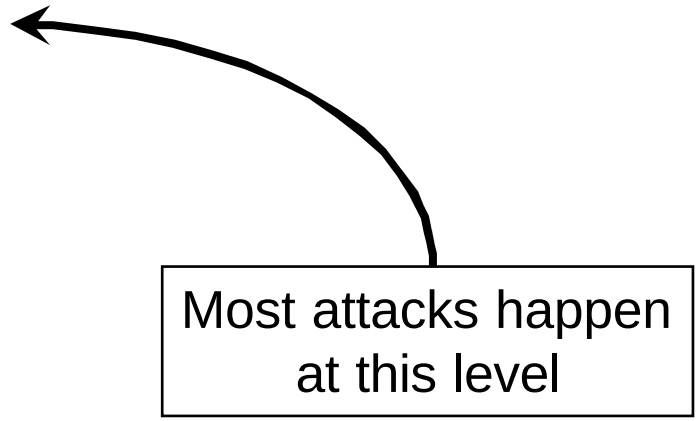
Just this is sufficient

- OPC
- PLC
- RTU
- ModBus
- IEC 60870
- ICCP
- HMI/MMI
- S5/S7
- Fieldbus
- IED
- TASE-2

This is all on the Internet

How does SCADA work?

- Multi-tier systems
- Physical measurement/control endpoints
  - RTU, PLC
  - Measure voltage, adjust valve, flip switch
- Intermediate processing
  - Usually based on commercial OS
  - VMS, Windows, Unix, Linux
- Communication infrastructure
  - Analog, Serial, Internet, Wi-Fi
  - Modbus, DNP3, OPC, ICCP
- Human Interface



Problems with SCADA

- SCADA = no authentication
  - What is the “identity” of an automated system?
  - OPC on Windows requires anonymous login rights for DCOM
  - How can policies such as “change your password monthly” be applied to automated systems running unattended for years?
  - How do you manage rights for each person?
- SCADA = no patching
  - Systems never needed patches in the past
  - install a system, replace it in 10 years
  - large window of vulnerability

Problems with SCADA

- SCADA = ~~not~~ connected to the Internet
  - often believed: not interconnected at all
  - found in reality: numerous uncontrolled connections
  - even unconnected networks get connected via dial-in or notebooks from support personnel
- SCADA = insecure design and implementation
  - simple passwords used by many people and never changed
  - anonymous FTP, Telnet without password
  - access limitations in control software are often not used

SCADA System security is different

	Information Technology	Control Networks
Risk Impact	Loss of data	Loss of production, equipment, life
Risk Management	Recover by reboot	Fault tolerance essential
	Safety is a non-issue	Explicit hazard analysis expected
Reliability	Occasional Failures tolerated	Outages intolerable
	Beta test in field acceptable	Thorough quality assurance testing expected
Performance	High throughput demanded	Modest throughput acceptable
	High delay and jitter accepted	High delay a serious concern
Security	Most sites insecure	Tight physical security
	Little separation among intranets on same site	Information systems network isolated from plant network
	Focus is central server security	Focus is edge control device stability

SCADA System security is different

Aspect of IT	Corporate IT	Process Control IT
Anti-virus	widely used	often difficult / impossible to deploy
Lifetime	3-5 years	5-20 years
Outsourcing	widely used	rarely used for operations
Patching	frequent (often daily)	slow (required vendor approval)
Change	frequent	rare
Time criticality	delays OK	critical, often safety dependent
Availability	outages OK (overnight)	24 / 7 / 365
Security skills and awareness	fairly good	poor
Security testing	widely used	must be used with care
Physical security	usually secure and manned	often remote and unmanned

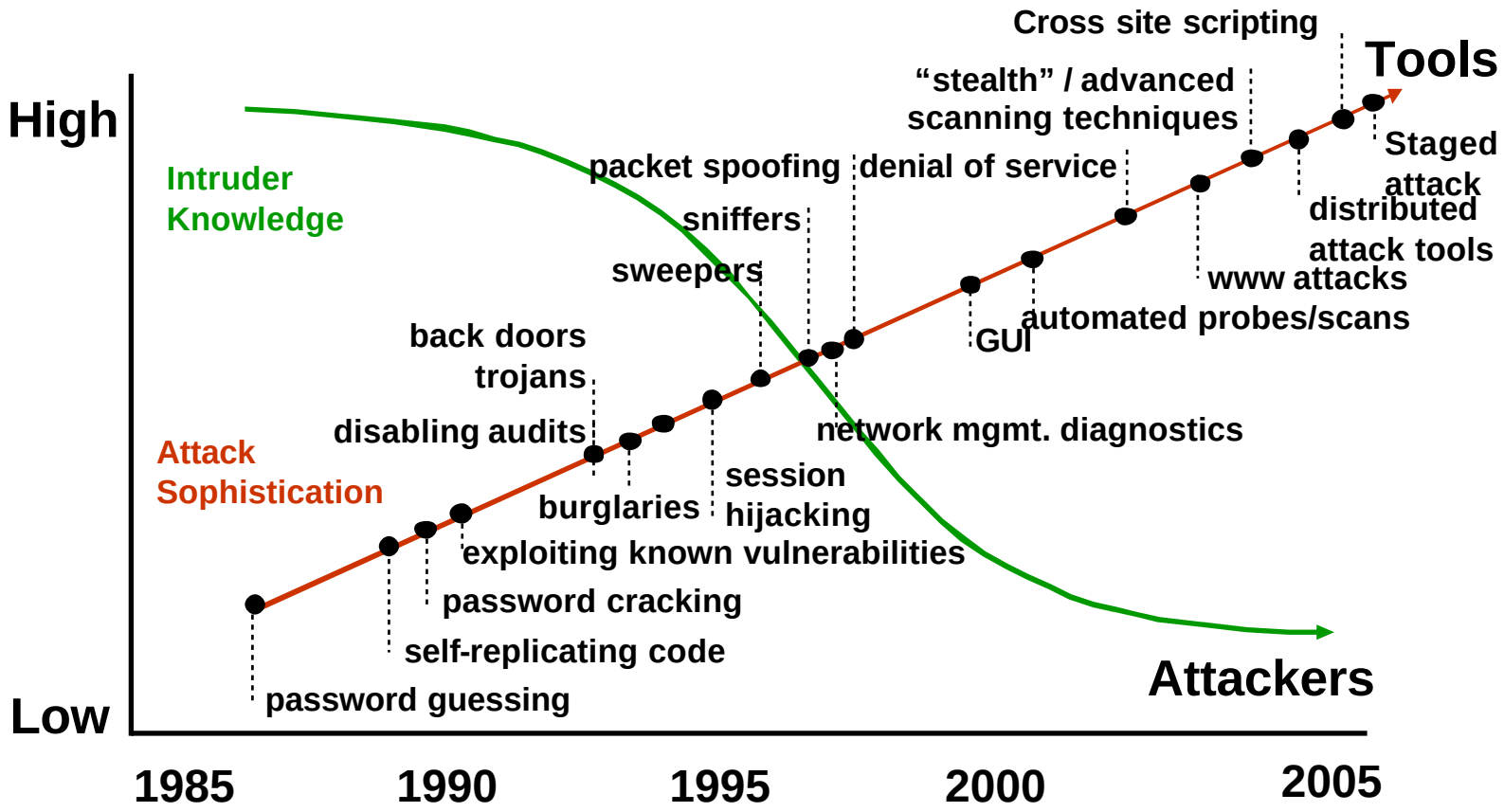
Standards for IT-Security in SCADA

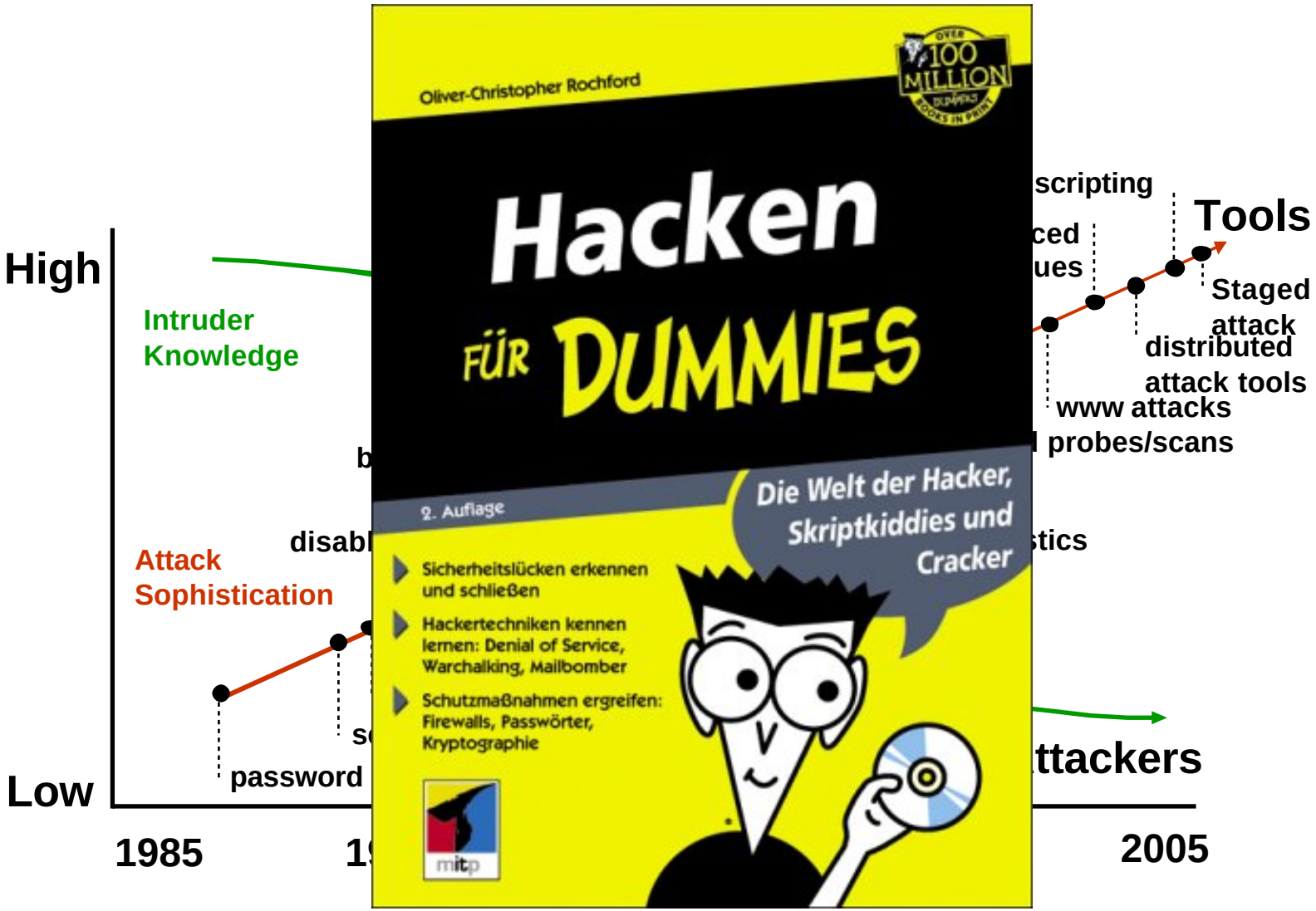
Standards	Title	Board
BS 7799/ISO 17799	Information Security Management	British Standards Institute / International Organization for Standardization
ISO 27001	Information Security Management	International Organization for Standardization
ISA SP99	Manufacturing and Control Systems Security	Instrumentation Systems and Automation
IEC 62443 (draft)	widely used	International Electrotechnical Commission
IEC 61784-4 (draft) (IEC SC65c WG13)	Digital Data Communications for Measurement and Control Network and System Security	International Electrotechnical Commission
NIST Process Control Security Requirements Forum (PCSRF)	System Protection Profiles (SPP) and Protection Profiles (PP) for Common Criteria (ISO 15408)	National Institute for Standards and Technology
NERC Cyber Security Standard	US IT-security standard for power plant operation	North American Electric Reliability Council
NISSC Practice Guide on Firewall Deployment for SCADA and Process Control Networks	Firewall Deployment for SCADA and Process Control Networks	UK National Infrastructure Security Coordination Centre
NIST Special Publication 800-40	Procedures for Handling Security Patches	National Institute for Standards and Technology

Real World Example

- Claim: “We are secure because the oil production network is completely separate from the rest of the corporate network”
- Flaw #1: network diagrams don’t match reality
  - It’s the desired configuration not the actual configuration
- Flaw #2: diagram obviously doesn’t match reality
  - Dial-in for remote support is in the office network not the production network, how can they connect?
- Flaw #3: notebooks
  - Notebooks are often used by support personnel to trace problems. Are the secured?
- Flaw #3: insecure production network
  - No patches, no segmentation, if one systems gets compromised, it can bring down everything

Hacking is easy

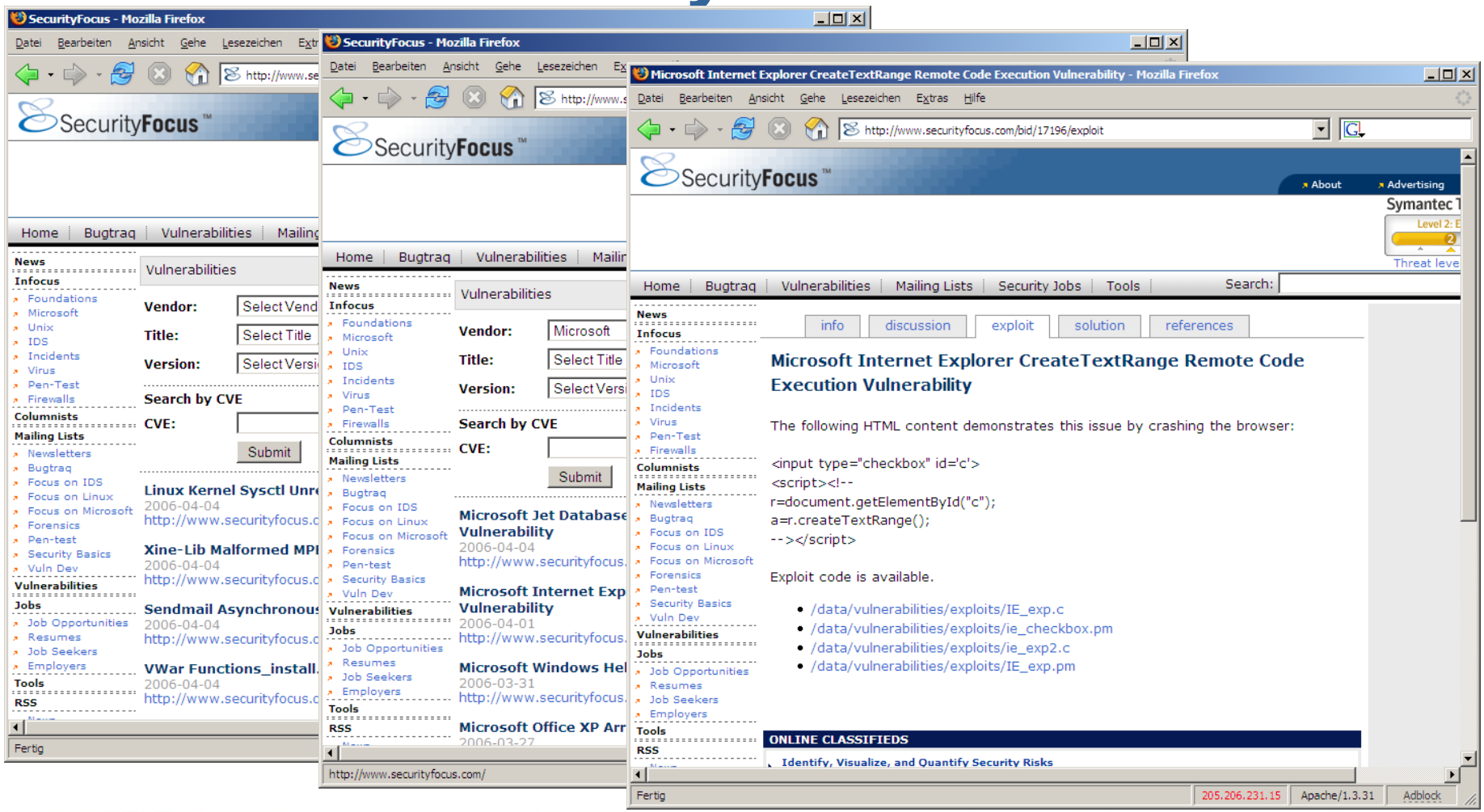



High
Intruder Knowledge
Attack Sophistication
Low
1985
2005
password
scripting
Tools
Staged attack
distributed attack tools
www attacks
probes/scans
ttackers
Oliver-Christopher Rochford
Hacken für DUMMIES
2. Auflage
Die Welt der Hacker, Skriptkiddies und Cracker
Sicherheitslücken erkennen und schließen
Hackertechniken kennen lernen: Denial of Service, Warchalking, Mailbomber
Schutzmaßnahmen ergreifen: Firewalls, Passwörter, Kryptographie
mitp

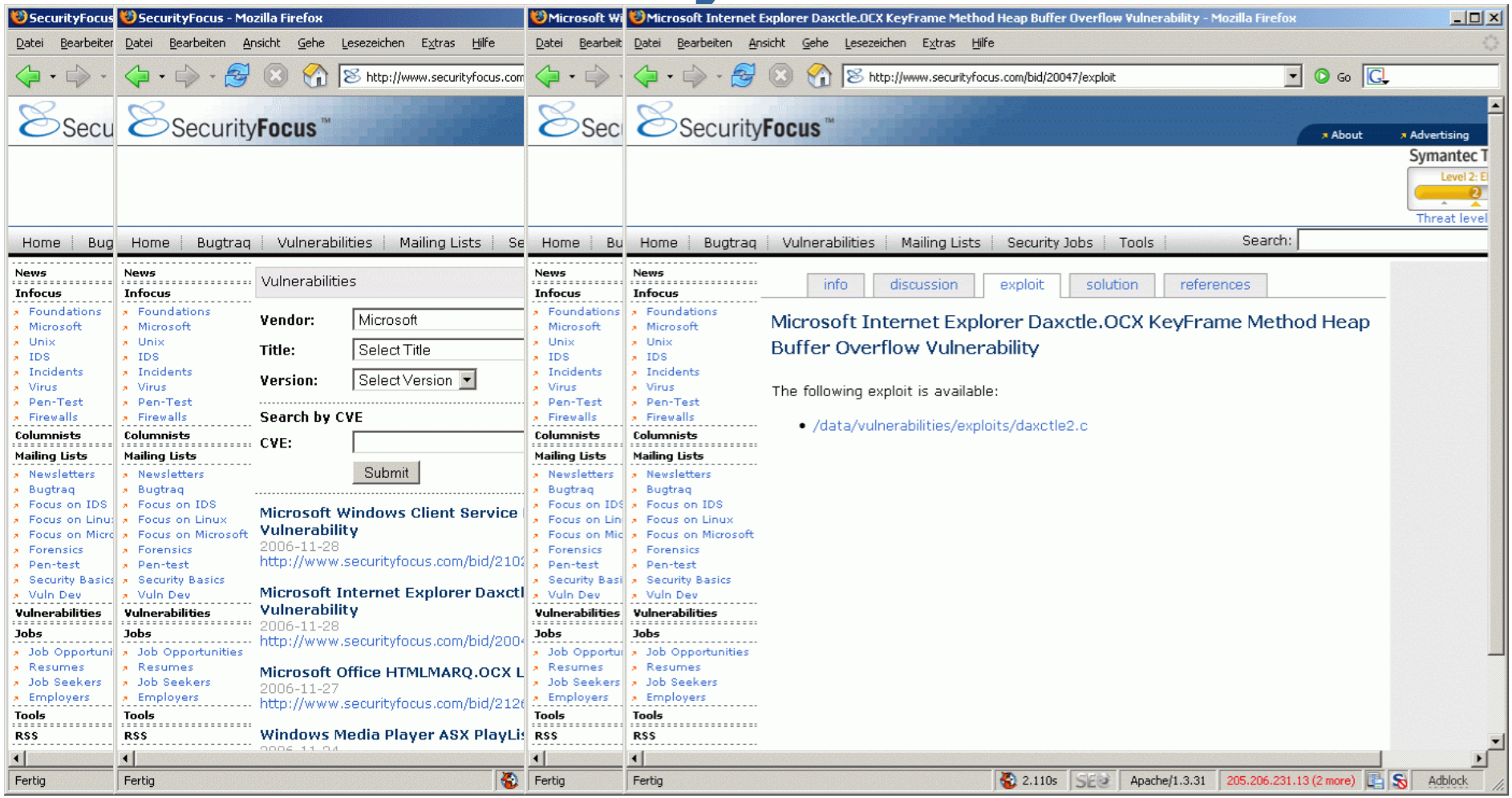
Example Hack

- This example break-in uses only publicly available free software and information
  - Nmap port scanner to identify the target OS
    (see: http//www.insecure.org/)
  - Nessus vulnerability scanner to identify the missing patches
    (see: http//www.nessus.org/)
  - Symantec SecurityFocus Vulnerability Database
    (see: http://www.securityfocus.com/bid/
    or: http://www.milw0rm.com/)
  - Metasploit Exploit Framework
    (see: http://www.metasploit.org/)
- Everyone can use these tools!

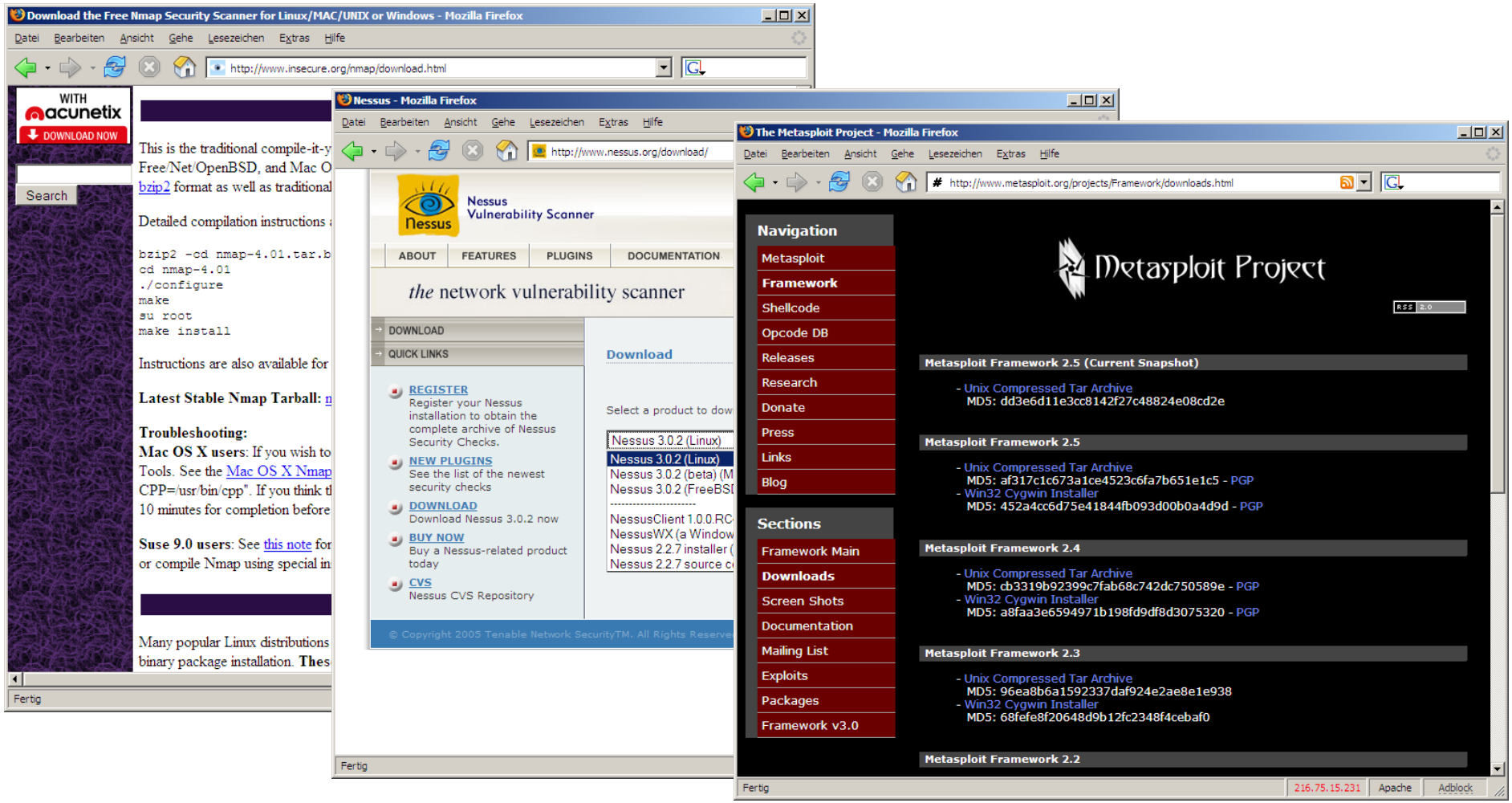
Free Vulnerability Databases – 04/04



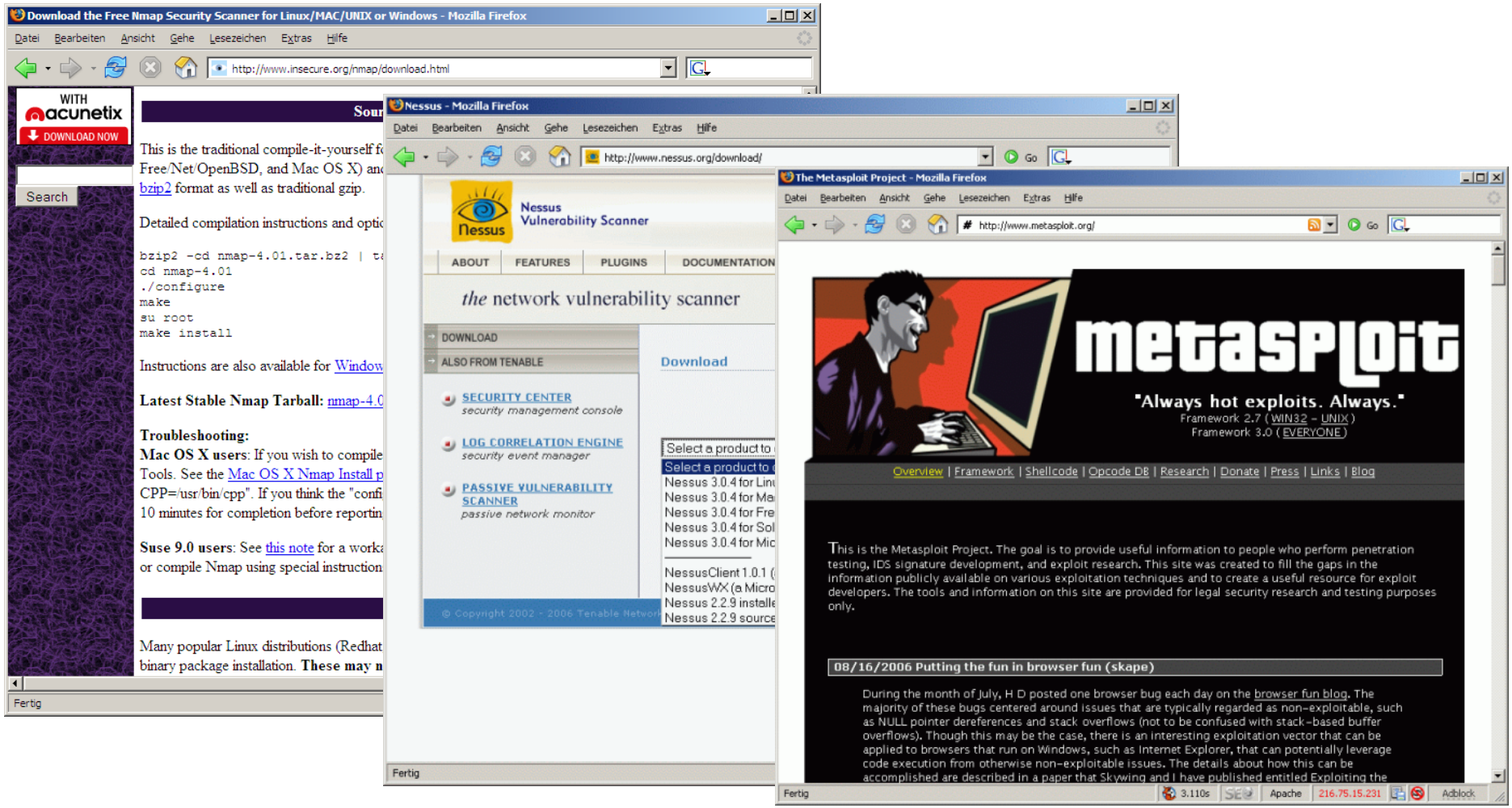
Free Vulnerability Databases – 28/11



Free Download of all Tools – 04/04



Free Download of all Tools – 28/11



Tools used in the Live Hack 29/11

- Some tools only work well with a Unix operating system, e.g. Nmap and Nessus
- For the live hacking today we use the following tools:
  - SuperScan4 from Foundstone (a division of McAfee, Inc.)
    (free download: http://www.foundstone.com/resources/freetools.htm)
  - Metasploit Exploit Framework
    (see: http://www.metasploit.org/)
  - SecurityFocus Vulnerability Database (a division of Symantec Corp.)
    (see: http://www.securityfocus.com/bid/
- The complete vulnerability scan with Nessus will be skipped due to time restraints

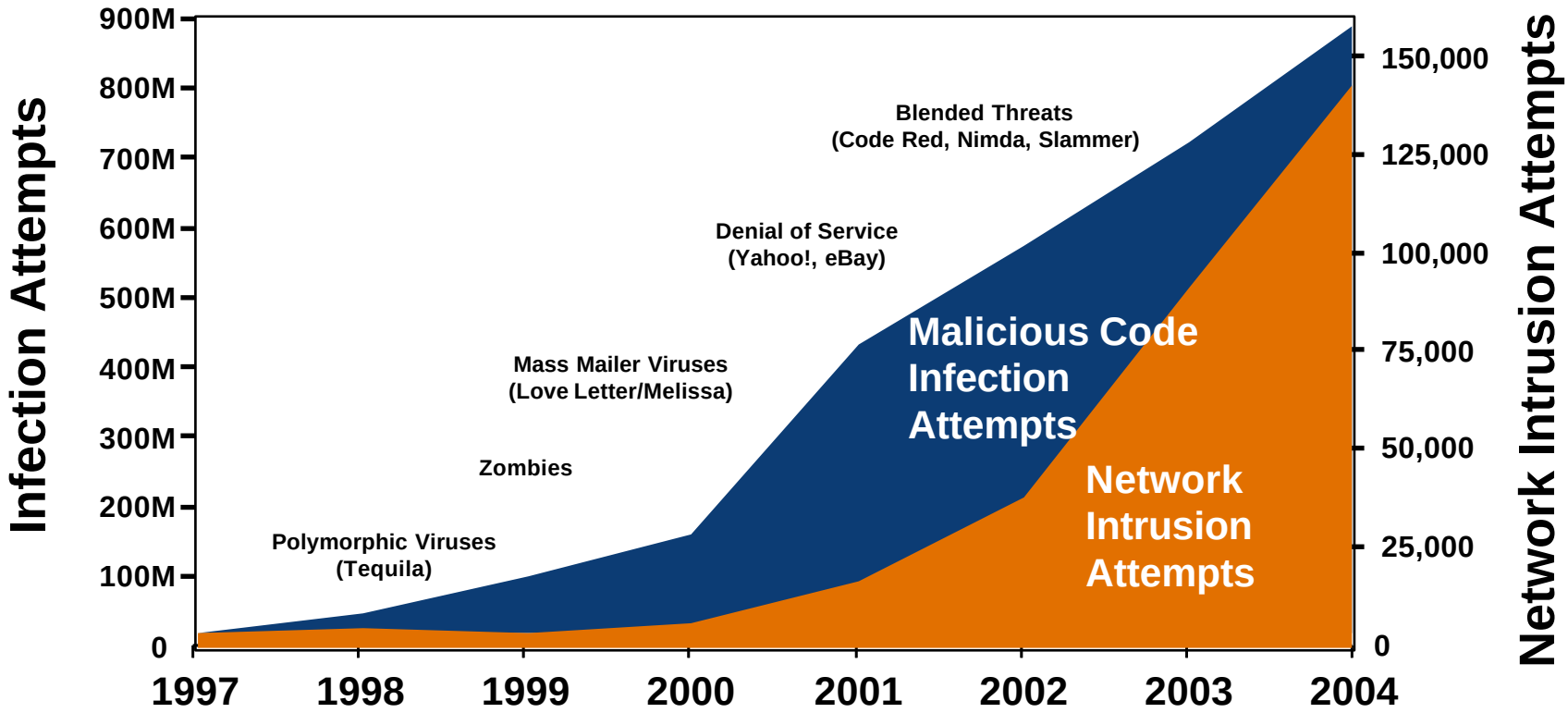
What's in the future

- Microsoft currently does a good job securing their systems
- There already is a trend to attack different parts in the operating system
  - backup software and anti-virus because agents are installed on all systems
  - completely new environments à production plants
- It is only a matter of time before automation systems will be attacked
- A good indicator are the SANS Top 20 Internet Security Vulnerabilities
  - see: http://www.sans.org/top20/

What's in the future

- 2006 was the year of application break-ins
  - widespread automated exploits for office applications but also backup software, anti-virus and personal firewalls
  - new and automated attacks against web applications
- 2007 will be the year of network components
  - exploits for router, switches and all the networking gear
  - Critical infrastructure like DNS will be targeted again
- 2008 will be the year of embedded and automation systems
  - many issues are fixed, new targets are required
  - these systems are finally connected to the networks

More attacks!



More viruses!

ICSA Labs Virus Prevalence Survey 2004

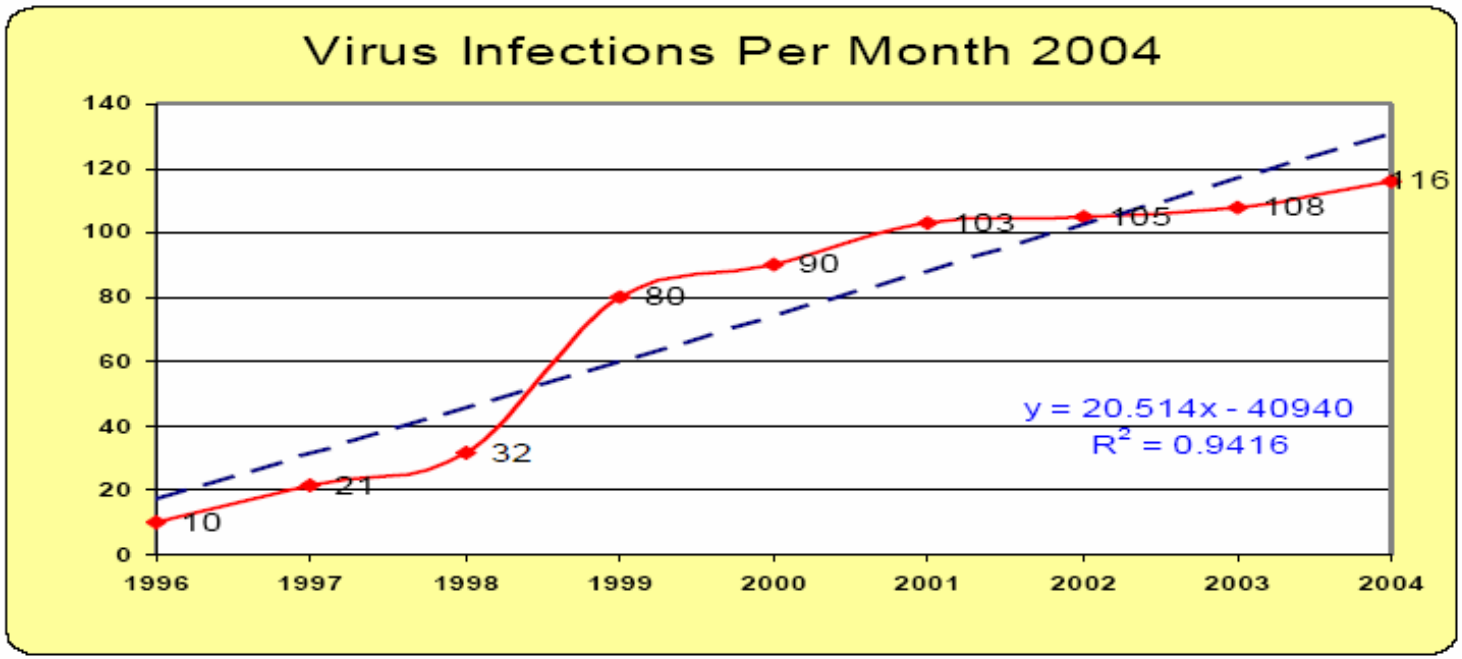


Figure 1: Infections per 1,000 PCs per month

New attack vectors!

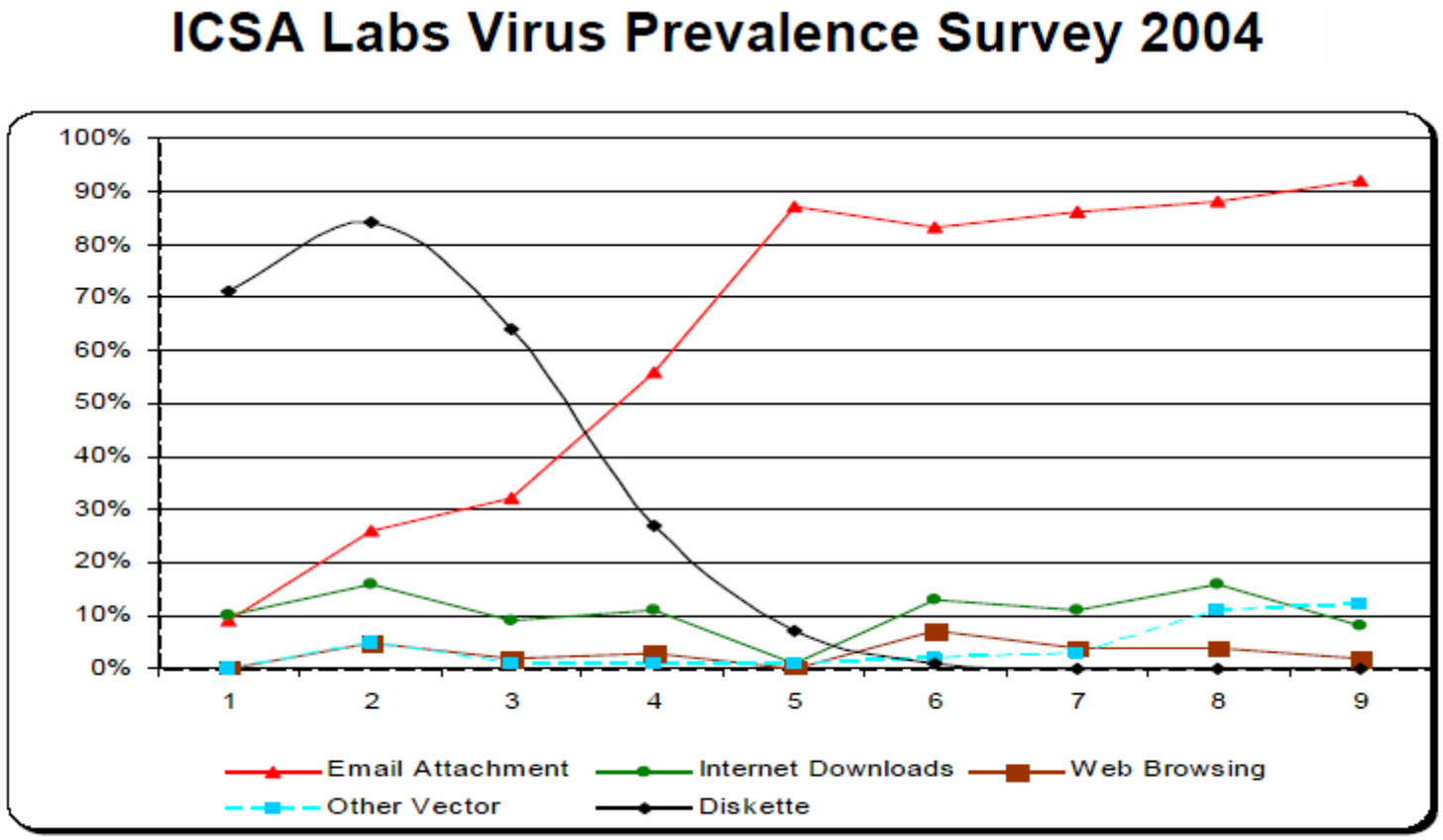


Figure 10: Virus encounter vectors

Shift in awareness necessary

- Control systems have become very similar to office environments
  à They need to be treated similar
- Control systems are interconnected to corporate networks or even the internet
  à They need the same (or even better) protection
- Shift in security awareness:
  - IT security should be part of the initial design process not an add-on later
  - IT security should be part of the standard maintenance procedures not only after an incident
  - Every employee is responsible for IT security

Awareness is Rising – Finally

- ISS gave a presentation on SCADA Security at the Black Hat Federal Conference in January 2006
- They found lot‘s of problems in widely used software …
  - OPC has many buffer overflows
  - OPC over DCOM is often very insecure
- … and while analyzing SCADA systems
  - SCADA systems usually have no authentication
  - SCADA systems are usually not patched

“You can go to the store and buy a book on pen-testing that will give you all the knowledge you need to cause a widespread power blackout!“

Multilayered approach necessary

- Protecting the infrastructure
  - Block access to sensitive parts of the infrastructure (e.g. rooms, buildings), often referred to as physical security
- Protecting IT-systems
  - Use anti-virus software and install patches to protect systems from viruses, worms and exploits
- Protecting networks
  - Use firewalls and filters for network segmentation
- Protecting applications and data
  - Use encryption and VPNs to protect data from unauthorized access
- User education
  - Train your employees to use and adopt IT security

Lessons learned

- IT security is becoming very important
  - Control networks are no longer isolated networks
  - Automation systems are no longer specialized platforms
  - They are “new” targets
  - They are “interesting” targets
- Hacking Tools are easy to use
  - Everybody can attack and break into systems
  - The tools are readily available
  - If you are not protected, you will be hacked
- **There is neither cause to panic nor cause to ignore the issue**

References

- Kevin Poulsen, Slammer worm crashed Ohio nuke plant network, http://www.securityfocus.com/news/6767
- SQL Slammer Worm Lessons Learned for Consideration by the Electricity Sector, North American Electric Reliability Council, http://www.esisac.com/publicdocs/SQL_Slammer_2003.pdf
- NRC Information Notice 2003-14, Potential Vulnerability of Plant Computer Network to Worm Infection, United States Nuclear Regulatory Commission, http://www.nrc.gov/reading-rm/doc-collections/news/2003/03-108.html
- Instrumentation, Systems and Automation Society (ISA), Security Technologies for Manufacturing and Control Systems, Technical Report ANSI/ISA-TR99.00.01-2004, ANSI/ISA-TR99.00.02-2004, March/April 2004, http://www.isa.org/
- International Electrotechnical Commission, Enterprise Network – Control Network Interconnection Profile (ECI), IEC/SC 65C/W 13 Draft v1.04, December 2004
- National Infrastructure Security Coordination Centre (NISCC), NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks, Revision 1.4, February 2005, http://www.niscc.gov.uk/niscc/docs/re-20050223-00157.pdf
- NIST, Procedures for Handling Security Patches, NIST Special Publication 800-40, August 2002, http://csrc.nist.gov/publications/nistpubs/

What NESEC can do

- Expertise in penetration testing of process control networks
- „Working and applicable“ concepts and solutions to secure production IT environments and PCNs
- Review of existing security concepts
- Development of “Best Practices” for PCNs

What can we do for you ???

NESEC
Gesellschaft für angewandte Netzwerksicherheit mbH

Thank you very much for your attendance
Your questions please …

Christian H. Gresser
NESEC GmbH
Lichtenbergstrasse 8
D-85748 Garching

Tel.: +49 89 5484-2130
Fax: +49 89 5484-2139
eMail: cgresser@nesec.de
Web: http://www.nesec.de/