Testimony of
Gerhard Eschelbeck, Ph.D.

CTO & VP of Engineering, Qualys, Inc.

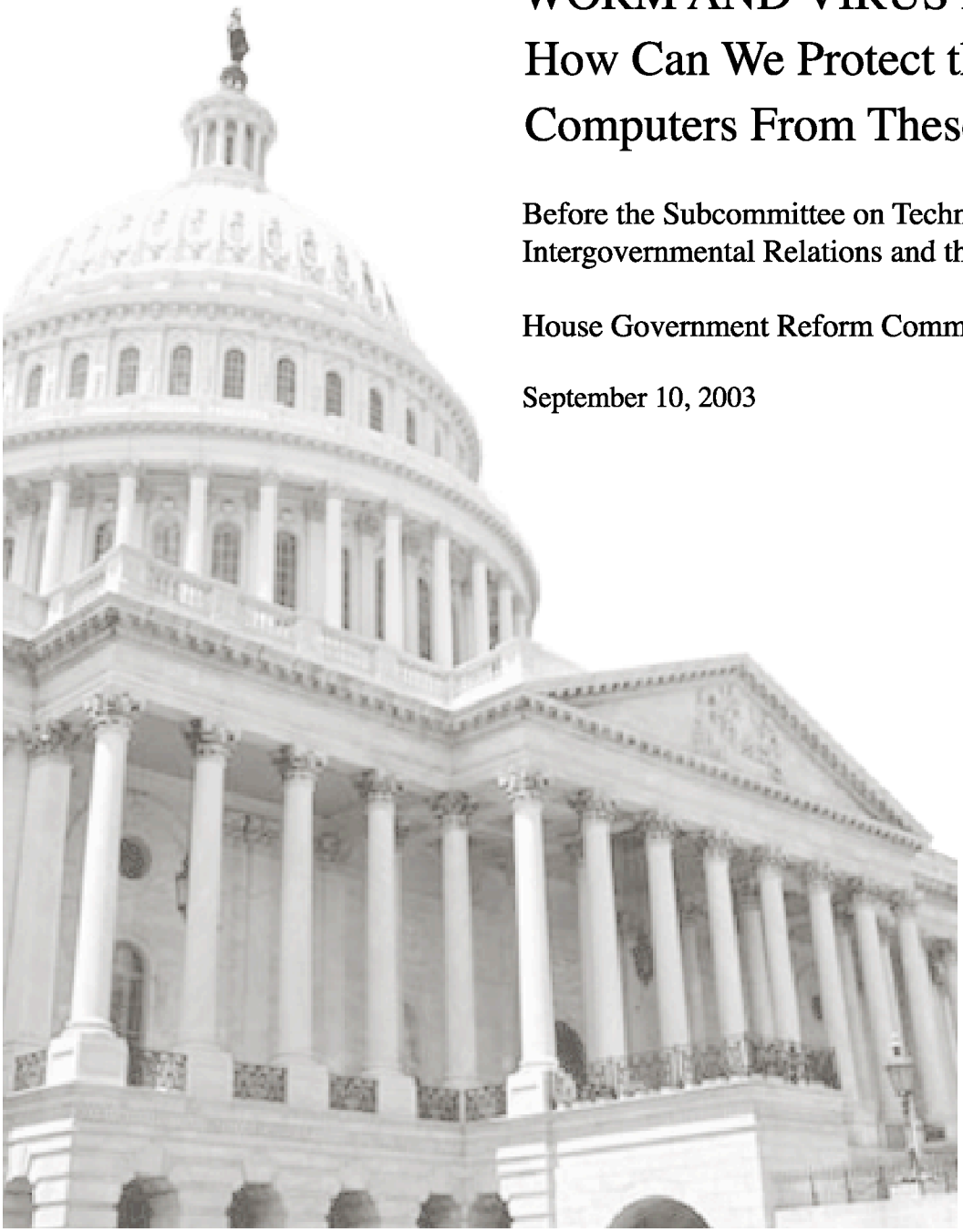
as presented to the United States Congress

"WORM AND VIRUS DEFENSE: How Can We Protect the Nation's Computers From These Threats?"

Before the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census

House Government Reform Committee

September 10, 2003



QUALYS
SECURITY ON-DEMAND

MR. CHAIRMAN and Members of the Subcommittee: I am Gerhard Eschelbeck, Chief Technology Officer and Vice President of Engineering at Qualys, Inc. Thank you for the invitation to testify about my research on network vulnerabilities and how we can protect the nation's computers from new threats.

The business of my company gives us a front row seat to new threats against applications, networked computers and communications systems. Responding to the growing sophistication of security threats, Qualys has developed an infrastructure for automated vulnerability detection. Such automation allows us to produce security audits immediately and cost-effectively over the Web for networks of all sizes. Based on our research and experience with network vulnerabilities, we believe the development of public policy for minimizing network-based attacks requires provisions for security automation to effectively protect against a new breed of automated attack technologies.

I have just analyzed 1.24 million network vulnerabilities found by our scanning service during a recent 18-month period. This vast data pool demonstrates that known risks are far more prevalent than anyone has imagined. Analytical data also demonstrates a new breed of automated, Internet-born viruses and worms that mock traditional security defenses.

Data for my analysis were a statistically significant sample anonymously drawn from 1.5 million security audit scans made by organizations worldwide. We learned four themes that I call the "Laws of Vulnerabilities":[1]

#1 is "Half-life" – The half-life of critical vulnerabilities is 30 days and doubles with lowering degrees of severity. In other words, for even the most dangerous vulnerabilities, it still takes organizations 30 days to patch 50% of the vulnerable systems, leaving them exposed for a significant period of time.

#2 is "Prevalence" – Half of the most prevalent and critical vulnerabilities are being replaced by new vulnerabilities each year. The continuous discovery of most dangerous and widespread vulnerabilities creates an ever changing window of exposure to computers and networks.

#3 is "Persistence" – The lifespan of some vulnerabilities is unlimited. Old risks recur partly due to new deployment of PCs and servers with faulty unpatched software.

#4 is "Exploitation" – 80% of vulnerability exploits are available within 60 days of public announcements of those vulnerabilities. Such rapid availability of exploits creates a significant exposure for organizations until they patch all their vulnerable systems.

[1] See "The Laws of Vulnerabilities" at www.qualys.com/laws.

Data for the four themes document the persistent ability of attackers to gain full control of systems – including access to highly sensitive information such as financial data and intellectual property. Automating defenses against these threats is crucial because human-based efforts are not working. In each case of recent damaging strikes, we've had advance warning – weeks, even months – to prepare for known vulnerabilities. Yet attackers still were able to hit hundreds of thousands of PCs and servers, crippling vital businesses and services and causing other havoc. Internet-borne risks threaten everyone including consumers, commercial, and public organizations and local, state, and federal governments.

AUTOMATED ATTACKS BRING MORE RISK

Risks to network and system security are increasing because their triggers are becoming automatic, requiring no human action to deliver destructive payloads. Consequently, security incidents reported to the CERT Coordination Center are soaring. Incidents rose 2,099 percent from 1998 through 2002 – an average annual compounded rate of 116 percent. Incidents reported during January through June of 2003 already totaled 93 percent of incidents for all of 2002![2]

The nature of these risks is changing dramatically. Earlier "First Generation" threats are virus-type attacks spread with email and file sharing. They require human action to trigger replication and spreading, such as opening an infected file attachment. Examples are the Melissa Macro virus, the LoveLetter VBScript worm, and, most recently, the SoBig virus.

"Second Generation" threats comprise active worms leveraging system and application vulnerabilities. Penetration occurs without requiring user action. Replication, identification, and targeting of new victims are automatic. Blended threats are common, such as incorporating viruses and Trojans. Recent examples are the Slapper worm (9/02), the SQL Slammer worm (1/03), and the Blaster worm (8/03).

NEW CHALLENGES POSED BY RISKS OF THE FUTURE

A "Third Generation" of threats is now posing trouble. We've already seen the potential for damage. On January 25, 2003, the SQL Slammer worm rapidly hit more than 75,000 hosts running Microsoft SQL Server, crippling Internet operations in South Korea, disabling cash machines at a major U.S. bank, disrupting 911 call center operations near Seattle, and causing other disruptions worldwide. SQL Slammer was the fastest worm ever, infecting more than 90 percent of vulnerable hosts within 10 minutes. It reached a full scanning rate of more than 55 million scans per second after just three minutes.[3] SQL Slammer, although lacking much of the potential of Third Generation Threats, demonstrated the aggressiveness of hyper-propagation.

The recent Blaster worm had many signs of a Third Generation Threat. Exploiting the Microsoft DCOM remote procedure call vulnerability, Blaster infected more than 100,000 systems per hour at its peak. Microsoft published news of the vulnerability including a patch on July 16, 2003. Within two days Qualys' automated scanning service ranked this security vulnerability in the global Top 10 list of most prevalent vulnerabilities. The DCOM vulnerability ranked #1 after just four days, making it the most prevalent vulnerability ever. Following the Laws of

---

[2] See www.cert.org/stats/cert_stats.html.

[3] See "Inside the Slammer Worm," IEEE Security & Privacy, July/August 2003 at http://computer.org/security/v1n4/j4wea.htm.

Vulnerabilities, Blaster and its derivatives appeared three weeks later causing disruption and significant financial impact.

Third Generation threats contain five characteristics:

#1 – Faster Damage by Quick Propagation. By pre-compiling and cataloging vulnerable targets in advance, Third Generation threats strike faster – preventing timely intervention by security administrators. Strikes can be finished in just minutes.

#2 – Leverage Known & Unknown Vulnerabilities. New attacks continue to exploit known vulnerabilities. Pre-compiling techniques used in Third Generation attacks will also enable use of obscure vulnerabilities, including those that are unknown to the broader security community.

#3 – Employ Multiple Attack Vectors. Simultaneous targets will include new technologies lacking strong security, such as Instant Messaging, wireless network infrastructure and voice-over-IP systems. Third Generation attacks will also leverage polymorphic techniques for concealment and encryption to prevent discovery during attack.

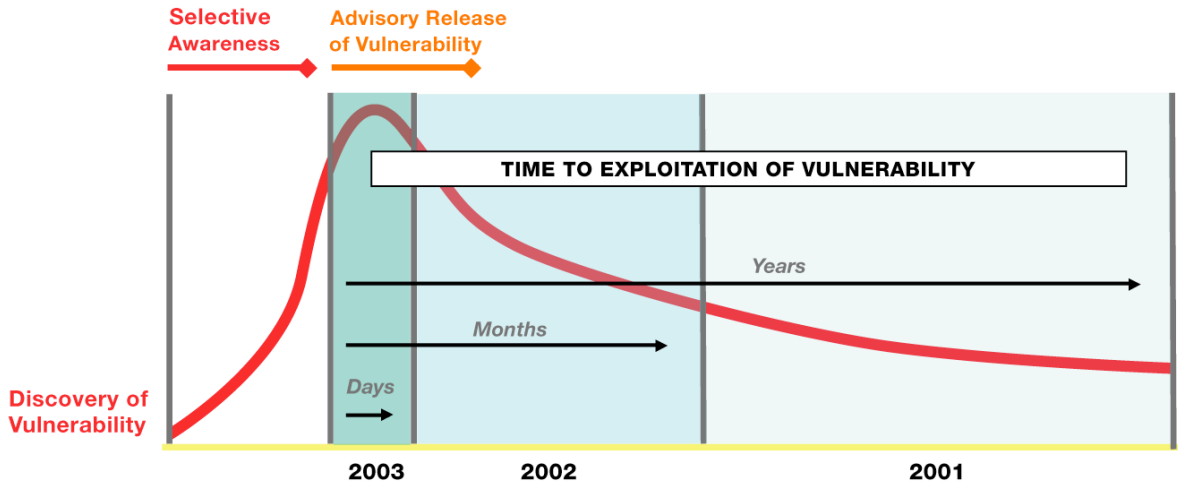
#4 – Use Active Payloads. Active payloads have specific targets such as a geographic area, an industry or a particular company. Blaster's payload was to create a distributed denial of service attack against Microsoft Corporation starting Aug. 16, 2003. Active payloads may be covert, holding back attacks for a future date or silently perform malicious actions such as modifying or deleting content on a victimized system.

#5 – Attack Inside Perimeter Defenses. Third Generation threats are shredding traditional defenses of the network perimeter. Worms like SQL Slammer and Blaster target covert channels to penetrate internal networks, such as compromising home PCs used for office connectivity and by other means.

TAKING CHARGE WITH AUTOMATED DEFENSES

Persistence and hyper-propagation are important considerations in creating public policy for network security. In the past, the discovery/attack lifecycle was a year or more from the advent of discovering a vulnerability to widespread exploitation. Urgency is now rising from a shorter discovery/attack cycle – SQL Slammer happened six months after discovery, Nimda was four months, Slapper was six weeks, and the most recent Blaster and Nachi worms came just three weeks after news of the vulnerability.

The diagram below illustrates compression of the discovery/attack lifecycle.



Source: Qualys, as published in *SC Magazine*, July 2003

Public policy for network security should strongly encourage use of automation as an equal-force response to automated tools used by attackers. Automating defense strategies include:

- **Regular Security Audits of Networks and Systems**. New automated audit solutions identify everything susceptible to attack, identify and prioritize vulnerabilities, and match them with appropriate remedies, such as patches and new security-device configuration settings.
- **Keep Antivirus Software Up-to-Date**. Server- and client- based solutions for automatic detection and cleansing of systems provide protection only if continuously updated.
- **Timely Patch Management**. Automated audit scanners can quickly identify which systems need urgent care and facilitate a timely and consistent remediation process.
- **Ongoing Evaluation of Security Policy**. Trend analysis with automated scanning solutions provides data for ensuring that security systems help meet the ever-changing nature of attack threats; thus enabling organizations to take control of their network security, adhere to security best practices and help comply with regulatory legislations.

CONCLUSION

In summary, network security attacks are increasing in number and sophistication. My research demonstrates that many vulnerabilities linger, sometimes without end. New and evolving attacks are capable of spreading faster than any possible human response effort. Protecting our networks is a continuous process of eliminating critical vulnerabilities on a regional, national and international scale. Public policy for network security should demand the timely and complete detection of security vulnerabilities with automated techniques and rapid application of remedies. These measures effectively thwart new automated attacks and protect the continuity of critical network-based applications and services.

Thank you again for the opportunity to testify to the Subcommittee. I look forward to your questions.

Gerhard Eschelbeck, Ph.D.